DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy 6-1: Desktop Work Stations

1. References.

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

   i. 4ID Policy # 5: Passwords.

   j. 4ID Policy # 11: Rules of Behavior.

2. Purpose of Policy:

   a. This policy addresses methods and practices to manage Information Assurance (IA) risks inherent in desktop work station computers connected to, or storing information retrieved from, 4ID supported Automated Information Systems (AIS) and communications resources.

   b. The current 4ID AIS communications environment interleaves trusted and public communications resources. This environment presents inherent IA risks to trusted military information resources regardless of whether connecting devices are fixed station desktop computers located on secured military facilities or whether they are portable devices using dial-in or wireless connectivity.

   c. Desktop workstation computers provide certain types of IA risks. Users must be aware of these risks and take the necessary steps to minimize such exposure.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

a. Commanders, directors, and supervisors at all levels shall ensure that subordinate personnel are aware of their individual responsibilities to protect these valuable resources and use them in an authorized and effective manner. Refer to the 4ID policy on Rules of Behavior.

b. Users of automated information systems (AIS) will use automated resources responsibly and abide by normal standards of professional and personal conduct at all times.

c. All 4ID personnel shall report suspected unauthorized activity to their respective Information Assurance Manager (IAM), Information Assurance Network Manager/Officer (IANM/O), or Information Assurance Security Officer (IASO).

5. Policy - Desktop Workstation Computers:

a. Only desktop workstation computers owned by the U.S. Army shall be provided connectivity to the 4ID automated information systems infrastructure. Violation of this will result in confiscation until the hard drive is wiped/purged by IA personnel.

b. Install IAVA patches and corrective patches as required.

c. Each workstation shall be configured with user ID and password access controls that are compliant with the 4ID password policy.

d. Approved password protected screen savers shall be configured to protect unattended workstations logged into the network from casual unauthorized access. The time period for workstation inactivity before the password protected screen saver is activated may vary depending on the individual user preference; however, it shall not be in excess of 1 hour.

e. Workstations used to process highly sensitive information shall not have writable, removable media devices installed. The network server shall be used to store data that requires backing up.

f. Users and their supervisors are responsible for defining the type of data to be backed up to network file servers from assigned desktop workstations, and are responsible for backing up the data to the respective server. System Administrators shall be responsible for backing up the file servers in accordance with the server policy.

g. Workstations shall be configured to be C2 compliant or as close thereto as technically possible. The current Army security baseline configurations for desktop workstation operating systems are developed and maintained by Regional Computer Emergency Response Team – Europe (RCERT-C) and can be found at https://www.rcert-c.army.mil/

h. Microsoft product baselines can be found at https://iassure.usareur.army.mil/security/microsoft/.

i. Changes to the configuration baseline shall be in accordance with the 4ID Configuration Management Plan (CMP) and coordinated and/or approved by the 4ID Configuration Control Board (CCB).

6. Non-compliance:

Managers will be held accountable for defining desktop requirements and ensuring that all are configured in compliance with the above policies.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding